2023 年四川省职业院校技能大赛（高等职业教育）

“信息安全管理与评估”样题

竞赛需要完成三个阶段的任务，分别完成三个模块，总分共计 1000 分。三个模块内容和分值分别是：

1.第一阶段：模块一 网络平台搭建与设备安全防护（180 分钟，300 分）。

2.第二阶段：模块二 网络安全事件响应、数字取证调查、应用程序安全（180 分钟，300 分）。

3.第三阶段：模块三 网络安全渗透、理论技能与职业素养（180 分钟，400 分）。

【注意事项】

1.第一个阶段需要按裁判组专门提供的U 盘中的“XXX-答题模板”提交答案。

第二阶段请根据现场具体题目要求操作。

第三阶段网络安全渗透部分请根据现场具体题目要求操作，理论测试部分根据测试系统说明进行登录测试。

2.所有竞赛任务都可以由参赛选手根据基础设施列表中指定的设备和软件完成。

第一阶段

模块一 网络平台搭建与设备安全防护

一、竞赛内容

第一阶段竞赛内容包括：网络平台搭建、网络安全设备配置与防护，共 2 个子任务。

竞赛阶段	任务阶段	竞赛任务	竞赛时间	分值
第一阶段 网络平台搭建与设备安全防护	任务 1	网络平台搭建	XX:XX-XX:XX	50
	任务 2	网络安全设备配置与防护		250
总分				**300**

二、竞赛时长

本阶段竞赛时长为 180 分钟，共 300 分。

三、注意事项

第一阶段请按裁判组专门提供的 U 盘中的“XXX-答题模板”中的要求提交答案。

选手需要在 U 盘的根目录下建立一个名为“GWxx”的文件夹（xx 用具体的工位号替代），所完成的“XXX-答题模板”放置在文件夹中作为竞赛结果提交。

例如：08 工位，则需要在 U 盘根目录下建立“GW08”文件夹，并在“GW08”文件夹下直接放置第一个阶段的所有“XXX-答题模板”文件。

【特别提醒】

只允许在根目录下的“GWxx”文件夹中体现一次工位信息，不允许在其它文件夹名称或文件名称中再次体现工位信息，否则按作弊处理。

五、赛项环境设置

1.网络拓扑图

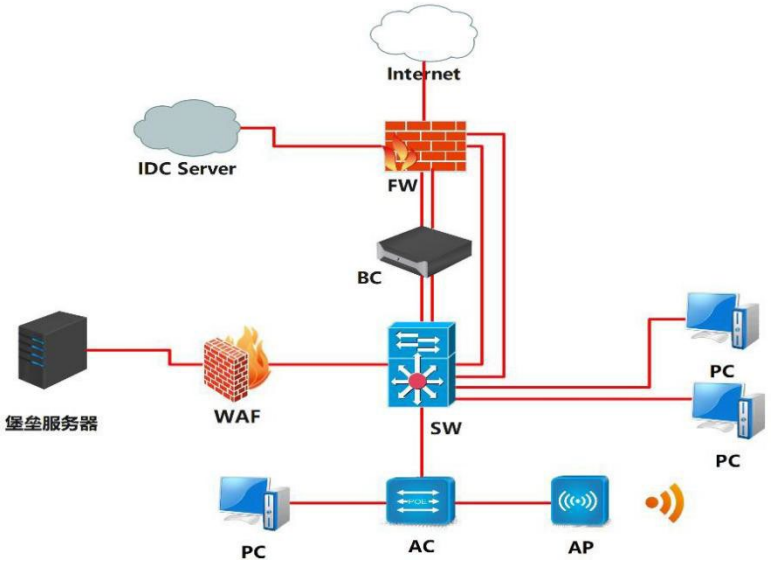

图 1 网络拓扑图

2.IP 地址规划表

设备名称	接口	IP 地址	对端设备
防火墙 FW	ETH0/1-2（AG1）	AG1.113 10.1.0.254/30 （Trust 安全域）	SW ETH1/0/1 SW ETH1/0/2
		AG1.114 10.2.0.254/30 （Trust 安全域）	
	ETH0/3	10.3.0.254/30 （Trust 安全域）	BC ETH3
	ETH0/4	10.4.0.254/30 （Trust 安全域）	BC ETH4
	ETH0/5	10.100.18.1/27	IDC SERVER

设备名称	接口	IP 地址	对端设备
		（untrust 安全域）	10.100.18.2
	ETH0/6	200.1.1.1/28 （untrust 安全域）	INTERNET
	Loopback1	10.11.0.1/24 （Trust 安全域）	-
	Loopback2	10.12.0.1/24 （Trust 安全域）	
	Loopback3	10.13.0.1/24 （Trust 安全域）	
	Loopback4	10.14.0.1/24 （Trust 安全域）	
路由交换机 SW	VLAN 40 ETH1/0/4-8	172.16.40.62/26	PC2
	VLAN 50 ETH1/0/3	172.16.50.62/26	PC3
	VLAN 51 ETH1/0/23	10.51.0.254/30	BC ETH5
	VLAN 52 ETH1/0/24	10.52.0.254/24	WAF ETH3
	VLAN 113 ETH1/0/1	VLAN113 OSPF 10.1.0.253/30	FW ETH0/1
	VLAN 114 ETH1/0/2	VLAN114 OSPF 10.2.0.253/30	FW ETH0/2
	VLAN 117 ETH E1/0/17	10.3.0.253/30	BC ETH1
	VLAN 118 SW ETH E1/0/18	10.4.0.253/30	BC ETH2
	ETH1/0/20	VLAN 100 192.168.100.1/30 2001::192:168:100:1/112 VLAN115 OSPF 10.5.0.254/30 VLAN116 OSPF 10.6.0.254/30	AC ETH1/0/20
无线控制器 AC	ETH1/0/20	VLAN 100 192.168.100.2/30 2001::192:168:100:2/112 VLAN 115 10.5.0.253/30 VLAN 116 10.6.0.253/30	SW ETH1/0/20
	VLAN 30 ETH1/0/3	172.16.30.62/26	PC1
	无线管理 VLAN VLAN 101	需配置	AP

设备名称	接口	IP 地址	对端设备
	ETH1/0/21		
	VLAN 10	需配置	无线 1
	VLAN 20	需配置	无线 2
网络日志系统 BC	ETH1	网桥	FW
	ETH3		SW ETH E1/0/17
	ETH2	网桥	FW
	ETH4		SW ETH E1/0/18
	ETH5	10.51.0.253/30	SW ETH E1/0/23
Web 应用防火墙 WAF	ETH3	10.52.0.253/30	SW ETH E1/0/24
	ETH4		堡垒服务器

第一阶段 任务书

任务 1 网络平台搭建（50 分）

题号	网络需求
1	按照 IP 地址规划表，对防火墙的名称、各接口 IP 地址进行配置
2	按照 IP 地址规划表，对三层交换机的名称进行配置，创建 VLAN 并将相应接口划入 VLAN, 对各接口 IP 地址进行配置
3	按照 IP 地址规划表，对无线交换机的名称进行配置，创建 VLAN 并将相应接口划入 VLAN,对接口 IP 地址进行配置
4	按照 IP 地址规划表，对网络日志系统的名称、各接口 IP 地址进行配置
5	按照 IP 地址规划表，对 Web 应用防火墙的名称、各接口 IP 地址进行配置

任务 2 网络安全设备配置与防护（250 分）

1.SW 开启 telnet 登录功能，用户名 skills01，密码 skills01，密码呈现需加密。

2.总部交换机SW 配置简单网络管理协议，计划启用V3 版本，V3 版本在安全性方面做了极大的扩充。配置引擎号分别为 62001；创建认证用户为skills01，采用 3des 算法进行加密，密钥为：skills01，哈希算法为SHA，密钥为：skills01；加入组ABC，采用最高安全级别；配置组的读、写视图分别为：2023_R、2023_W；当设备有异常

时，需要使用本地的VLAN100 地址发送Trap 消息至网管服务器10.51.0.203，采用最高安全级别。

3.接入SW Eth4，仅允许IP 地址 172.16.40.62-80 为源的数据包为合法包，以其它IP 地址为源地址，交换机直接丢弃。

4.为减少内部ARP 广播询问VLAN 网关地址，在全局下配置 SW 每隔 300S 发送免费ARP。

5.勒索蠕虫病毒席卷全球，爆发了堪称史上最大规模的网络攻击，通过对总部核心交换机SW 所有业务VLAN 下配置访问控制策略实现双向安全防护。

6.SW 配置IPv6 地址，使用相关特性实现VLAN50 的 IPv6 终端可自动从网关处获得IPv6 有状态地址。

7.AC 配置IPv6 地址，开启路由公告功能，路由器公告的生存期为 2 小时，确保VLAN30 的 IPv6 终端可以获得IPv6 无状态地址。

8.AC 与 SW 之间配置RIPng，使PC1 与 PC3 可以通过IPv6 通信。

9.IPv6 业务地址规划如下，其它IPv6 地址自行规划：

业务	IPV6 地址
VLAN30	2001:30::254/64
VLAN50	2001:50::254/64

10.FW、SW、AC 之间配置OSPF area 0 开启基于链路的MD5 认证，密钥自定义,传播访问INTERNET 默认路由。

11.FW 与 SW 建立两对IBGP 邻居关系，使用AS 65500，FW 上 loopback1-4 为模拟AS 65500 中网络，为保证数据通信的可靠性和负载，完成以下配置，要求如下：

- SW 通过BGP 到达loopback1,2 网路下一跳为 10.3.0.254；
- SW 通过BGP 到达loopback3,4 网络下一跳为 10.4.0.254。

12.FW 与 SW 建立两对IBGP 邻居关系，使用AS 65500，FW 上loopback1-4 为模拟AS 65500 中网络，为保证数据通信的可靠性和负载，通过BGP 实现到达loopback1,2,3,4 的网络冗余，请完成配置。

13.FW 与 SW 建立两对IBGP 邻居关系，使用AS 65500，FW 上loopback1-4 为模拟AS 65500 中网络，为保证数据通信的可靠性和负载，使用IP 前缀列表匹配上述业务数据流，请完成配置。

14.FW 与 SW 建立两对IBGP 邻居关系，使用AS 65500，FW 上loopback1-4 为模拟AS 65500 中网络，为保证数据通信的可靠性和负载，完成以下配置，使用 LP 属性进行业务选路，只允许使用 route-map 来改变LP 属性、实现路由控制，LP 属性可配置的参数数值为：200。

15.配置使总部VLAN50 业务的用户访问IDC SERVER 的数据流经过FW 10.1.0.254, IDC SERVER 返回数据流经过FW 10.2.0.254，且对双向数据流开启所有安全防护，参数和行为为默认。

16.在端口ethernet1/0/7 上，将属于网段 172.16.40.62/26 内的报文带宽限制为 10M 比特/秒，突发 4M 字节，超过带宽的该网段内的报文一律丢弃。

17.在 FW 上配置，连接LAN 接口开启PING 等所有管理方式，连接Internet 接口关闭所有管理方式，配置trust 区域与 Untrust 之间的安全策略且禁止从外网访问内网的任何设备。

18.总部VLAN 业务用户通过防火墙访问Internet 时，复用公网IP： 200.1.1.28/28，保证每一个源IP 产生的所有会话将被映射到同一个固定的IP 地址，当有流量匹配本地址转换规则时产生日志信息， 将匹配的日志发送至 10.51.0.253 的 UDP 2000 端口。

19.为了合理利用网络出口带宽，需要对内网用户访问 Internet 进行流量控制，园区总出口带宽为 200M，对除无线用户以外的用户限

制带宽，每天上午 9:00 到下午 6:00 每个IP 最大下载速率为 2Mbps，上传速率为 1Mbps。

20.配置L2TP VPN，名称为VPN，满足远程办公用户通过拨号登陆访问内网，创建隧道接口为tunnel 1、并加入untrust 安全域，地址池名称为AddressPool，LNS 地址池为10.100.253.1/24-10.100.253.100/24，网关为最大可用地址，认证账号skills01,密码skills01。

21.Internet 端有一分支结构路由器，需要在总部防火墙FW 上完成以下预配，保证总部与分支机构的安全连接：防火墙 FW 与 Internet 端路由器 202.5.17.2 建立GRE 隧道，并使用IPSec 保护GRE 隧道，保证分支结构中 2.2.2.2 与总部VLAN40 安全通信。

22.Vlan30 内的工作人员涉及到商业机密，因此在FW 上配置不允许vlan30 内所有用户访问外网。

23.配置出于安全考虑，无线用户访问因特网需要采用认证，在防火墙上配置 Web 认证，采用本地认证，用户名为 test，test1，test2，密码为 123456。

24.已知原AP 管理地址为 10.81.0.0/15，为了避免地址浪费请重新规划和配置IP 地址段，使用原 AP 所在网络进行地址划分，请完成配置。

25.已知原AP 管理地址为 10.81.0.0/15，为了避免地址浪费请重新规划和配置IP 地址段，现无线用户 VLAN 10 中需要 127 个终端，无线用户VLAN 20 需要 50 个终端，请完成配置。

26.已知原AP 管理地址为 10.81.0.0/15，为了避免地址浪费请重新规划和配置IP 地址段，要求完成在 AC 上配置DHCP，管理 VLAN 为 VLAN101,为 AP 下发管理地址，网段中第一个可用地址为AP 管

理地址，最后一个可用地址为 AC 管理地址，保证完成 AP 二层注册；为无线用户VLAN10,20 下发IP 地址，最后一个可用地址为网关。

27.在 NETWORK 下配置SSID，需求如下：

● NETWORK 1 下设置SSID 2023skills-2.4G，VLAN10，加密模式为wpa-personal,其口令为skills01；

● NETWORK 20 下设置SSID 2023skills-5G，VLAN20 不进行认证加密,做相应配置隐藏该SSID。

28.配置一个SSID 2023skills_IPv6，属于VLAN21 用于IPv6 无线测试，用户接入无线网络时需要采用基于WPA-personal 加密方式，其口令为“skills01”，该网络中的用户从AC DHCP 获取IPv6 地址，地址范围为：2001:10:81::/112。

29.NETWORK 1 开启内置portal+本地认证的认证方式，账号为GUEST 密码为 123456,保障无线信息的覆盖性，无线AP 的发射功率设置为 90%。禁止MAC 地址为 80-45-DD-77-CC-48 的无线终端连接。

30.2023skills-5G 最多接入 20 个用户，用户间相互隔离，并对2023skills-5G 网络进行流控，上行速率 1Mbps，下行速率 2Mbps。

31.在 AC 上配置使radio 1 的射频类型为IEEE 802.11b/g,并且设置 RTS 的门限值为 256 字节，当MPDU 的长度超过该值时，802.11 MAC 启动RTS/CTS 交互机制。

32.在 AC 上配置一条基于SSID 时间点时周一 0 点到 6 点的禁止用户接入的策略（限时策略）。

33.通过配置防止多AP 和 AC 相连时过多的安全认证连接而消耗CPU 资源，检测到AP 与 AC 在 10 分钟内建立连接 5 次就不再允许继续连接，两小时后恢复正常。

34.配置所有无线接入用户相互隔离，Network 模式下限制每天 0 点到 6 点禁止终端接入，开启ARP 抑制功能。

35.在公司总部的BC 上配置，设备部署方式为透明模式。增加非admin 账户skills01，密码skills01，该账户仅用于用户查询设备的日志信息和统计信息；要求对内网访问 Internet 全部应用进行日志记录。

36.BC 上配置用户认证识别功能。

37.在公司总部的BC 上配置，在工作日（每周一到周五上班）期间针对所有无线网段访问互联网进行审计，如果发现访问互联网的无线用户就断网，不限制其他用户在工作日（每周一到周五上班）期间访问互联网。

38.使用BC 对内网所有上网用户进行上网本地认证，要求认证后得用户 3 小时候重新认证，并且对HTTP 服务器 172.16.10.45 的 80 端口进行免认证。

39. BC 配置应用“即时聊天”，在周一至周五 9：00-21：00 监控内网中所有用户的微信账号使用记录，并记录数据。

40.在 BC 上配置激活NTP，本地时区+8:00，并添加 NTP 服务器名称清华大学，域名为s1b.time.edu.cn。

41. BC 配置内容管理，对邮件内容包含“比赛答案”字样的邮件，记录且邮件报警。

42.BI 监控周一至周五工作时间VLAN40 用户使用“迅雷”的记录，每天工作时间为 9:00-18:00。

43.在公司总部的 WAF 上配置，设备部署方式为透明模式。要求对内网HTTP 服务器 172.16.10.45/32 进行安全防护。

44.方便日志的保存和查看，需要在把 WAF 上攻击日志、访问日志、DDoS 日志以JSON 格式发给IP 地址为 172.16.10.200 的日志服务器上。

45.在 WAF 上配置基础防御功能，开启SQL 注入、XXS 攻击、信息泄露等防御功能，要求针对这些攻击阻断并发送邮件告警。

46.为防止www.2023skills.com 网站资源被其他网站利用，通过 WAF 对资源链接进行保护，通过 Referer 方式检测，设置严重级别为中级，一经发现阻断并发送邮件告警。

47.在公司总部的 WAF 上配置，编辑防护策略，定义 HTTP 请求体的最大长度为 256，防止缓冲区溢出攻击。

48.对公司内网用户访问外网进行网页关键字过滤，网页内容包含“暴力”“赌博”的禁止访问。

49.为了安全考虑，无线用户移动性较强，访问因特网时需要实名认证，在 BC 上开启web 认证使用http 方式，采用本地认证，密码账号都为web2023。

50.在 WAF 上保护HTTP 服务器上的www.2023skills.com 网站爬虫攻击，从而影响服务器性能，设置严重级别为高级，一经发现攻击阻断并发送邮件告警。

第二阶段

模块二 网络安全事件响应、数字取证调查、应用程序安全

一、竞赛内容

第二阶段竞赛内容包括：网络安全事件响应、数字取证调查和应用程序安全。

竞赛阶段	任务阶段		竞赛任务	竞赛时间	分值
第二阶段 网络安全事件响应、数字取证调查和应用程序安全	网络安全事件响应	任务 1	应急响应	XX:XX-XX:XX	70
	数字取证调查	任务 2	操作系统取证		40
		任务 3	网络数据包分析		50
		任务 4	计算机单机取证		60
	应用程序安全	任务 5	恶意代码分析		50
		任务 6	代码审计		30
总分					**300**

二、竞赛时长

本阶段竞赛时长为 180 分钟，共 300 分。

三、注意事项

1.本部分的所有工作任务素材或环境均已放置在指定的计算机上，参赛选手完成后，填写在电脑桌面上“信息安全管理与评估竞赛-第二阶段答题卷”中。

2.选手的电脑中已经安装好 Office 软件并提供必要的软件工具（Tools 工具包）。

【特别提醒】

竞赛有固定的开始和结束时间，选手必须决定如何有效的分配时间。请阅读以下指引！

1.当竞赛结束，**离开时请不要关机**；

2.所有配置应当在重启后有效；

3.除了 CD-ROM/HDD/NET 驱动器，请不要修改实体机的配置和虚拟机本身的硬件设置。

第二阶段 任务书

任务描述

随着网络和信息化水平的不断发展，网络安全事件也层出不穷，网络恶意代码传播、信息窃取、信息篡改、远程控制等各种网络攻击 行为已严重威胁到信息系统的机密性、完整性和可用性。因此，对抗 网络攻击，组织安全事件应急响应，采集电子证据等技术工作是网络 安全防护的重要部分。现在，A 集团已遭受来自不明组织的非法恶意攻击，您的团队需要帮助 A 集团追踪此网络攻击来源，分析恶意攻击行为的证据线索，找出操作系统和应用程序中的漏洞或者恶意代码， 帮助其巩固网络安全防线。

本模块主要分为以下几个部分：

- 网络安全事件响应；
- 数字取证调查；
- 应用程序安全。

第一部分 网络安全事件响应

任务 1 应急响应（70 分）

A 集团的 WebServer 服务器被黑客入侵，该服务器的 Web 应用系统被上传恶意软件，系统文件被恶意软件破坏，您的团队需要帮助该公司追踪此网络攻击的来源，在服务器上进行全面的检查，包括日志信息、进程信息、系统文件、恶意文件等，从而分析黑客的攻击行为，

和残留的关键证据信息。

本任务素材清单：Server 服务器虚拟机

受攻击的Server 服务器已整体打包成虚拟机文件保存，请选手自行导入分析。

虚拟机用户名：root，密码：123456，若题目中未明确规定，请使用默认配置。

请按要求完成该部分工作任务，答案有多项内容的请用换行分隔。

任务 1 应急响应		
序号	任务要求	答案
1	提交攻击者的两个内网 IP 地址	
2	提交网站管理员用户的用户名与密码	
3	提交黑客得到MySQL 服务的root 账号密码的时间（格式：dd/MM/yyyy:hh:mm:ss）	
4	查找黑客在 Web 应用文件中写入的恶意代码，提交文件绝对路径	
5	查找黑客在 Web 应用文件中写入的恶意代码，提交代码的最简形式（格式：<?php xxxx?>）	
6	分析攻击者的提权手法，提交攻击者通过哪一个指令成功提权	
7	服务器内与动态恶意程序相关的三个文件绝对路径	
8	恶意程序对外连接的目的 IP 地址	

第二部分 数字取证调查

任务 2 操作系统取证（40 分）

A 集团某电脑系统感染恶意程序，导致系统关键文件被破坏，请分析 A 集团提供的系统镜像和内存镜像，找到系统镜像中的恶意软件，分析恶意软件行为。

本任务素材清单：操作系统镜像、内存镜像（*.dump、*.img）

请按要求完成该部分的工作任务。

任务 2 操作系统取证		
序号	任务要求	答案
1	提交恶意进程名称（两个）	
2	被破坏的文件位置	
3	加密数据的内存地址	
4	原文件内容	
5	分析恶意程序行为	

任务 3 网络数据包分析（50 分）

A 集团的网络安全监控系统发现有恶意攻击者对集团官方网站进行攻击，并抓取了部分可疑流量包。请您根据捕捉到的流量包，搜寻出网络攻击线索，并分析黑客的恶意行为。

本任务素材清单：捕获的网络数据包文件（*.pcapng）

请按要求完成该部分的工作任务，答案有多项内容的请用换行分隔。

任务 3 网络数据包分析		
序号	任务要求	答案
1	提交恶意程序传输协议 （只提交一个协议，两个以上视为无效）	
2	恶意程序对外连接目标 IP	
3	恶意程序加载的 dll 文件名称	
4	解密恶意程序传输内容	
5	分析恶意程序行为	

任务 4 计算机单机取证（60 分）

对给定取证镜像文件进行分析，搜寻证据关键字（线索关键字为“evidence 1”“evidence 2”……“evidence 10”，有文本形式也有图片形式，不区分大小写），请提取和固定比赛要求的标的证据文件，并按样例的格式要求填写相关信息，证据文件在总文件数中所占比例不低于 15%。取证的信息可能隐藏在正常的、已删除的或受损的文件中，您

可能需要运用编码转换技术、加解密技术、隐写技术、数据恢复技术，还需要熟悉常用的文件格式（如办公文档、压缩文档、图片等）。

本任务素材清单：取证镜像文件

请根据赛题环境及现场答题卡任务要求提交正确答案。

任务 4 计算机单机取证		
证据编号	**原始文件名（不包含路径）**	**镜像中原文件 Hash 码（MD5，不区分大小写）**
evidence 1		
evidence 2		
evidence 3		
evidence 4		
evidence 5		
evidence 6		
evidence 7		
evidence 8		
evidence 9		
evidence 10		

第三部分 应用程序安全

任务 5 恶意程序分析（50 分）

A 集团发现其发布的应用程序文件遭到非法篡改，您的团队需要协助A 集团对该恶意程序样本进行逆向分析、对其攻击/破坏的行为进行调查取证。

本任务素材清单：恶意程序代码

请按要求完成该部分的工作任务。

任务 5 恶意程序分析		
序号	任务内容	答案
1	请提交素材中的恶意应用回传数据的 url 地址	
2	请提交素材中的恶意代码保存数据文件名称（含路径）	
3	请描述素材中恶意代码的行为	
4	.....	

任务 6 代码审计（30 分）

代码审计是指对源代码进行检查，寻找代码存在的脆弱性，这是一项需要多方面技能的技术。作为一项软件安全检查工作，代码安全审查是非常重要的一部分，因为大部分代码从语法和语义上来说是正确的，但存在着可能被利用的安全漏洞，你必须依赖你的知识和经验来完成这项工作。

本任务素材清单：源文件

请按要求完成该部分的工作任务。

任务 6 代码审计		
序号	任务内容	答案
1	请指出存在安全漏洞的代码行	
2	请指出可能利用该漏洞的威胁名称	
3	请提出加固修改建议	
4	.....	

第三阶段

模块三 网络安全渗透、理论技能与职业素养

一、竞赛内容

第三阶段竞赛内容是：网络安全渗透、理论技能与职业素养。本阶段分为两个部分。第一部分主要是在一个模拟的网络环境中实现网络安全渗透测试工作，要求参赛选手作为攻击方，运用所学的信息收集、漏洞发现、漏洞利用等渗透测试技术完成对网络的渗透测试；并且能够通过各种信息安全相关技术分析获取存在的 flag 值。第二部分是在理论测试系统中进行考核。

竞赛阶段	任务阶段		竞赛任务	竞赛时间	分值
第三阶段网络安全渗透、理论技能与职业素养	网络安全渗透	第一部分：网站	任务 1～任务 3	XX:XX-XX:XX	45
		第二部分：应用系统	任务 4～任务 5		30
		第三部分：应用服务器 1	任务 6～任务 13		165
		第四部分：应用服务器 2	任务 14		30
		第五部分：应用服务器 2	任务 15		30
	第六部分：理论技能与职业素养				100
总分					**400**

二、竞赛时长

本阶段竞赛时长为 180 分钟，其中网络安全渗透 300 分，理论技能与职业素养 100 分，共 400 分。

三、注意事项

通过找到正确的flag 值来获取得分，flag 统一格式如下所示：

flag{<flag 值 >}

这种格式在某些环境中可能被隐藏甚至混淆。所以，注意一些敏

感信息并利用工具把它找出来。

【特别提醒】部分 flag 可能非统一格式，若存在此情况将会在题目描述中明确指出flag 格式，请注意审题。

第三阶段 任务书

任务描述

在 A 集团的网络中存在几台服务器，各服务器存在着不同业务服务。在网络中存在着一定网络安全隐患，请利用您所掌握的渗透测试技术，通过信息收集、漏洞挖掘等渗透测试技术，完成指定项目的渗透测试，在测试中获取flag 值。网络环境参考样例请查看附录A。

本模块所使用到的渗透测试技术包含但不限于如下技术领域：

- 数据库攻击；
- 枚举攻击；
- 权限提升攻击；
- 基于应用系统的攻击；
- 基于操作系统的攻击；
- 逆向分析；
- 密码学分析；
- 隐写分析。

所有设备和服务器的IP 地址请查看现场提供的设备列表，请根据赛题环境及现场答题卡任务要求提交正确答案。

第一部分 网站（45 分）

任务编号	任务描述	答案	分值
任务 1	门户网站存在漏洞，请利用漏洞并找到 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 2	门户网站存在漏洞，请利用漏洞并找到 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 3	门户网站存在漏洞，请利用漏洞并找到 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		

第二部分 应用系统（30 分）

任务编号	任务描述	答案	分值
任务 4	应用系统存在漏洞， 请利用漏洞并找到 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 5	应用系统存在漏洞， 请利用漏洞并找到 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		

第三部分 应用服务器 1（165 分）

任务编号	任务描述	答案	分值
任务 6	请获取 FTP 服务器上对应的文件进行分析找出其中隐藏的 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 7	请获取 FTP 服务器上对应的文件进行分析找出其中隐藏的 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 8	请获取 FTP 服务器上对应的文件进行分析找出其中隐藏的 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 9	请获取 FTP 服务器上对应的文件进行分析找出其中隐藏的 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		

任务 10	请获取 FTP 服务器上对应的文件进行分析找出其中隐藏的 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 11	请获取 FTP 服务器上对应的文件进行分析找出其中隐藏的 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 12	请获取 FTP 服务器上对应的文件进行分析找出其中隐藏的 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 13	请获取 FTP 服务器上对应的文件进行分析找出其中隐藏的 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		

第四部分 应用服务器 2（30 分）

任务编号	任务描述	答案	分值
任务 14	应用系统服务器 10000 端口存在漏洞，获取 FTP 服务器上对应的文件进行分析，请利用漏洞找到 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		

第五部分 应用服务器 3（30 分）

任务编号	任务描述	答案	分值
任务 15	应用系统服务器 10001 端口存在漏洞，获取 FTP 服务器上对应的文件进行分析，请利用漏洞找到 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		

附录 A

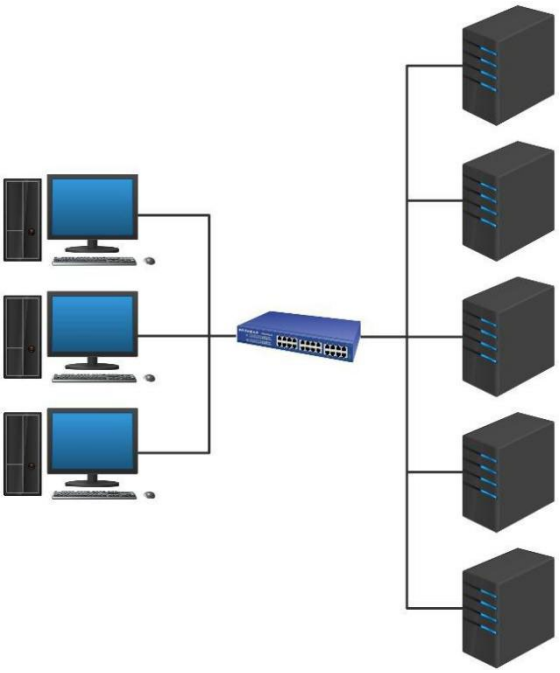

图 2 网络拓扑结构图